PUBLIC SECTOR LAW

# FAQ Datenschutz

**Eine Auswahl datenschutzrechtlicher Fragen für Schweizer Museen.**

## A– Spezifische Fragen

### 1) Veröffentlichung von Personendaten:

- **Inwieweit dürfen von einem Museum erfasste Personendaten veröffentlicht werden?**
- **Darf beispielsweise für Tagungen eine Teilnehmenden-Liste verteilt werden?**
- **Welche Informationen dürfen auf der Webseite oder im Geschäftsbericht veröffentlicht werden?**

Die Veröffentlichung von Personendaten stellt eine Datenbearbeitung dar (→ siehe dazu unter B – Allgemeine Erfordernisse des Datenschutzes, Frage 1). Als solche muss sie den Datenbearbeitungsgrundsätzen entsprechen (→ B – Allgemeine Erfordernisse des Datenschutzes, Frage 7).

Für Museen, die nicht als öffentliche Organe handeln (und daher dem Datenschutzrecht für Private des DSG[1] unterstehen) gilt Folgendes:

- Hier steht im Vordergrund, für welche *Zwecke* Personendaten erhoben wurden und ob die betroffenen Personen *informiert* wurden, dass die Personendaten veröffentlicht werden.
- *Information:*
    - Wenn man die betroffenen Personen von Anfang an (d.h. bei der Erhebung der Personendaten) *informiert* hat über die Veröffentlichung, so ist diese im Grundsatz zulässig.
- *Zweck*:
    - Wenn die Veröffentlichung der Daten von Anfang an für die betroffenen Person erkennbar war (z.B. indem im Anmeldeformular der Tagung steht «Vor Beginn der Tagung wird eine Teilnehmenden-Liste verschickt»), ist sie im Prinzip zulässig.
    - Wenn man die Daten aber aus ihrem ursprünglichen Bearbeitungskontext entnehmen will und sie zu einem anderen Zweck bearbeitet, stellt dies einen Verstoss gegen den Zweckbindungsgrundsatz dar.
    - Beispiel: Es soll eine Foto einer unabhängigen Kuratorin, die für die Erstellung einer Infotafel einer vergangenen Ausstellung gemacht wurde, nun im Newsletter des Museums erscheinen, der an 2'000 Personen geht und eine zukünftige andere Ausstellung bewirbt.
    - Damit diese Zweckänderung zulässig ist, muss sie gerechtfertigt werden. Dies kann namentlich getan werden, indem die *Einwilligung* der Kuratorin eingeholt wird. Diese muss nicht explizit und schriftlich geschehen (man könnte sie anrufen und ihr Einverständnis telefonisch einholen), es empfiehlt sich jedoch, das Einverständnis zu

[1] Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020, SR 235.1. Sofern in den FAQ das DSG erwähnt wird, wird auf die totalrevidierte Fassung Bezug genommen, die am 1. September 2023 in Kraft tritt.

dokumentieren, was am Einfachsten durch ein schriftlich unterzeichnetes Dokument geschieht.

Praktische Tipps:

- Die Kontaktdaten einer *Person, die im Museum eine bestimmte Rolle wahrnimmt* (z.B. Verantwortliche für einen Geschäftsbereich oder eine Ausstellung), dürfen mit den nötigen Angaben auf der Webseite des Museums oder im Geschäftsbericht veröffentlicht werden, sofern dies zur Erfüllung der Aufgabe der betreffenden Person gehört (z.B. weil sie in ihrer Funktion kontaktierbar sein muss).
- Angaben zu *Personen, die öffentlich bekannt sind* („Personen des öffentlichen Lebens", was bei Künstlerinnen und Künstlern oder Personen mit geschichtlicher Relevanz regelmässig der Fall sein dürfte), und die zu deren öffentlichem Wirken gehören, dürfen bearbeitet und daher auch veröffentlicht werden.
- Geht es darum, Fotos von Personen einer Tagung zu machen und zu veröffentlichen, ist (über die *Information* hinaus → siehe oben) eine eigentliche *Einwilligung* im Normalfall nicht nötig. Je nach Kontext kann es sich aber aus Beweisgründen empfehlen, eine nachweisbare Einwilligung zu dokumentieren (Unterschrift, Häkchen, das angekreuzt wird, etc.).

Weiter zu beachten:

- *Sicherheit*: Es ist zu prüfen, wie Daten jeweils adäquat gesichert werden können. Z.B. kann die gesamte Sammlung von Fotos von Teilnehmenden einer Tagung nur auf einem passwortgeschützten Bereich der Webseite zugänglich gemacht werden (anstatt frei aufgeschaltet), dasselbe gilt für eine Teilnehmenden-Liste.
- *Verhältnismässigkeit*: Will man in einer Publikation oder einem Newsletter Fotos eines Anlasses verwenden, so sind nach Möglichkeit solche zu wählen, die nicht übermässig viele direkt identifizierbare Gesichter zeigen. Zudem sind ggf. drei Bilder ausreichend anstatt deren 20 oder 30. Bei Teilnehmenden-Listen rechtfertigt es sich eher, Name, Vorname und E-Mail-Adresse zu veröffentlichen als auch noch die Adresse und die Telefonnummer.

Für Museen, die als öffentliche Organe handeln (und daher dem Datenschutzrecht für Bundesorgane des DSG bzw. kantonalem Datenschutzrecht unterstehen) ist darüber hinaus zu prüfen, ob die vorhandenen gesetzlichen Grundlagen für die Bekanntgabe der Personendaten ausreichend sind.

**2) Wie ist mit Personendaten in Bezug auf die Provenienzforschung umzugehen? Bzw. wie kann eine datenschutzkonforme Datenbearbeitung gewährleistet werden angesichts der Tatsache, dass verstorbene Personen keine Einwilligung mehr abgeben können?**

Stark vereinfacht gilt Folgendes:

| **Grundsätzlich zulässig** | **Im Einzelfall zu prüfen und mit Interessenabwägung oder Einwilligung zu lösen** |
|---|---|
| Provenienzforschung durch das Museum | Bekanntgabe an Dritte von Daten über noch lebende Personen |
| Bekanntgabe von Personendaten von Personen, die vor sehr langer Zeit verstorben sind | Bekanntgabe an Dritte von Daten verstorbener Personen, wenn die Angehörigen allenfalls einen Anspruch auf Ansehensschutz geltend machen könnten. |

Bei der Provenienzforschung ist das Datenschutzrecht nur anwendbar, solange das Museum Personendaten noch lebender Personen bearbeitet.

Mit dem Tod endet die Persönlichkeit und damit auch die Anwendung des Datenschutzrechts (dazu sogleich unten). Die Provenienzforschung, die sich auf Personendaten Verstorbener bezieht, stellt damit datenschutzrechtlich von Vorneherein kein Problem dar (siehe aber zum Andenkensschutz sogleich unten).

Hinweis: Für die Datenbearbeitung durch öffentliche Organe ist im Einzelfall zu prüfen, wie die Gesetzeslage aussieht und ob im Einzelfall Einschränkungen bestehen, die den nachfolgenden Ausführungen entgegenstehen.

Lebende Personen:

- *Recherchen des Museums als Datenbearbeitung*: Die Provenienzforschung durch das Museum selbst wird durch ein überwiegendes öffentliches oder privates Interesse gerechtfertigt sein (vgl. Art. 31 Abs. 1 DSG). Mit anderen Worten besteht ein Interesse daran, die rechtmässigen Eigentümerinnen oder Eigentümer zu kennen, was in der Waagschale gegenüber dem Recht der betroffenen Personen, keine Datenbearbeitungen über sich ergehen zu lassen, in den allermeisten Fällen ein grösseres Gewicht einnehmen wird. Damit ist Provenienzforschung grundsätzlich zulässig.
- *Bekanntgabe von Informationen an Dritte*: Fragen Drittpersonen nach der Herkunft von Werken oder Gegenständen, so wird die genaue rechtliche Abwicklung der Frage im Einzelfall je nach Konstellation und Gesetz zu prüfen sein. Als Grundregel geht es aber wiederum um eine Abwägung zwischen den Interessen der anfragenden Drittperson (erscheint ihr Interesse, die Personendaten zu kennen, legitim und nachvollziehbar?) und den Interessen derjenigen Person, die verhindern will, dass ihre Personendaten bekanntgegeben werden (auch hier: Erscheint ihr Interesse schützenswert?).
    - Ein privates Museum ohne öffentlichen Auftrag wird prüfen müssen, ob es für die Bekanntgabe der ersuchten Daten im Einzelfall ein überwiegendes Interesse gibt (etwa das Interesse der Öffentlichkeit, die Identität einer Person zu kennen). Ist dies nicht der Fall, sollten die Daten vorsichtshalber nur mit der Einwilligung der betreffenden Person herausgegeben werden.
    - Ein öffentliches Museum wird bereits im Rahmen der geltenden Öffentlichkeitsgesetze verpflichtet sein, die Abwägung vorzunehmen (vgl. für Bundesorgane Art. 36 Abs. 3 DSG). Besteht ein überwiegendes öffentliches Interesse daran, dass die Personendaten bekanntgegeben werden können (z.B., weil die Öffentlichkeit wissen sollte, dass eine Person Eigentümerin eines Werks ist oder war), so ist es zulässig, auch die dazugehörigen Personendaten herauszugeben.

Verstorbene Personen:

- Wie bereits oben erwähnt, sind die Daten verstorbener Personen datenschutzrechtlich nicht geschützt. Die *Bearbeitung von Daten durch das Museum im Rahmen seiner Recherchen* ist daher unproblematisch.
- Geht es um die Bekanntgabe an Dritte, können noch lebende Angehörige in gewissen Fällen einen Anspruch auf Schutz des Ansehens der verstorbenen Person geltend machen; dieser wird aber im Verlauf der Zeit abnehmen. Hier erfolgt wiederum eine Interessenabwägung.
- Als Faustregel gilt: Je weiter zurück der betreffende Zeitraum (bzw. der Tod der betroffenen Person) liegt, desto grosszügiger können Personendaten bekanntgegeben werden.

PUBLIC SECTOR LAW

## B – Allgemeine Erfordernisse des Datenschutzes

### 1) Wann muss das Datenschutzrecht beachtet werden?

Das Datenschutzrecht ist immer dann anwendbar, wenn *Personendaten bearbeitet* werden.

Bei *Personendaten* handelt es sich um Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. *Bestimmt* ist eine Person, wenn die Daten sie direkt identifizieren (z.B. Name und Vorname). *Bestimmbar* ist eine Person, wenn Daten aus Perspektive der Datenbearbeitenden oder in Kombination mit weiteren verfügbaren Informationen die Identifizierung dieser Person ermöglichen (bspw. Kundennummern in Verbindung mit einer Kundenliste oder Telefonnummern mit Zugang zu tel.search.ch).

Das *Bearbeiten* umfasst alle Handlungen im Zusammenhang mit Personendaten, z.B. das Erheben, Speichern, Verändern, Versenden, Löschen oder Anonymisieren. Also: Auch Daten, die auf einem Server unbenutzt «liegen», werden bearbeitet!

Allgemein gilt, dass die Begriffe Personendaten und Bearbeiten *sehr breit* sind. Das heisst, dass das Datenschutzrecht in den meisten Fällen zur Anwendung kommen wird.

### 2) Was ist Sinn und Zweck des Datenschutzes?

Jede Person hat ein Anrecht darauf, dass ihre personenbezogenen Daten geschützt werden. Der Datenschutz stellt den Schutz der Privatsphäre beim Umgang mit Personendaten als Grundrecht aller Menschen sicher.

Dazu sieht das Datenschutzrecht diverse Regeln für Datenbearbeitende (Unternehmen, öffentliche Organe oder Privatpersonen) im Umgang mit Personendaten vor. Weiter gibt es den betroffenen Personen, über die Daten bearbeitet werden, eine Reihe von Instrumenten an die Hand, um die Hoheit über ihre Daten zu behalten.

### 3) Wer muss innerhalb eines Museums das Datenschutzrecht beachten?

Alle! Das Handeln aller Mitarbeitenden, Organe und ihren Mitgliedern im Alltag ist für den Datenschutz zentral. Jedes Gesetz, jede Richtlinie, jede Weisung ist unnütz, wenn sie nicht im Arbeitsalltag umgesetzt werden.

Daher haben alle erwähnten Personen dafür zu sorgen, dass die Grundsätze des Datenschutzes sowie der Informationssicherheit im eigenen Tätigkeitsgebiet und im eigenen Arbeitsalltag umgesetzt werden.

Die einzuhaltenden Pflichten ergeben sich aus dem anwendbaren Datenschutzrecht sowie aus den innerhalb einer Organisation geltenden Weisungen und Richtlinien.

Wichtig ist aber, dass die oberste Verantwortung für die Umsetzung des Datenschutzes bei der Geschäftsleitung liegt: Es ist an ihr, die nötigen Massnahmen zu ergreifen und die Mitarbeitenden auszurüsten, damit diese den Datenschutz im Alltag umsetzen können.

## 4) Welches Datenschutzgesetz gilt für ein Museum?

Diese Frage muss für jedes Museum separat geklärt werden und es ist zwischen folgenden Konstellationen zu unterscheiden:

- Privatrechtlich organisierte Museen ohne öffentlichen Leistungsauftrag;
- Privatrechtlich organisierte Museen mit einem öffentlichen Leistungsauftrag des Bundes oder eines Kantons;
- Öffentlich-rechtlich organisierte Museen (öffentliche Organe des Bundes oder eines Kantons).

Für öffentliche Organe des kantonalen Rechts gilt das kantonale (Informations- und) Datenschutzrecht des jeweiligen Kantons (bspw. das Informations- und Datenschutzgesetz (IDG) des Kantons Zürich, LS 170.4)

Das Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) gilt für Private sowie Bundesorgane. Als *Private* gelten natürliche wie auch juristische Personen. Der Begriff des *Bundesorgans* umfasst die Bundesbehörden wie auch Private, die mit öffentlichen Aufgaben des Bundes betraut sind.

## 5) Ist auch europäisches Datenschutzrecht anwendbar?

Für gewisse Datenbearbeitungen kann auch die EU-Datenschutz-Grundverordnung (EU-DSGVO oder GDPR [Engl.]) eine Rolle spielen.

Die EU-DSGVO kann auch für Unternehmen oder Organisationen in der Schweiz zur Anwendung kommen, wenn a) diese natürlichen Personen in der EU Waren oder Dienstleistungen anbieten oder b) sie das Verhalten von natürlichen Personen in der EU beobachten, etwa durch weitgehendes Tracking des Surfverhaltens dieser Personen im Internet.

Für die Schweizer Museen kann dies dann der Fall sein, wenn bspw. elaboriertes Webtracking auf der Webseite eingesetzt wird (z.B. Google Analytics und Verknüpfung mit weiteren Datenbeständen) oder Angebote explizit an Personen im EU-Raum gerichtet werden (z.B. eine Weiterbildung wird in Deutschland oder Frankreich beworben und in EUR bepreist).

## 6) Was sind besonders schützenswerte Personendaten und was ist bei ihrer Bearbeitung zu beachten?

Besonders schützenswerte Personendaten haben aufgrund ihrer Sensitivität für die betroffene Person einen erhöhten Schutzbedarf. Dies ist der Fall, wenn Daten einen besonders tiefen Einblick in die Persönlichkeit und das Leben einer Person erlauben (Intimsphäre, Gesundheit), wenn sie auf risikoreiche Art bearbeitet werden oder wenn viele Daten miteinander kombiniert werden.

Das Datenschutzgesetz enthält strengere Anforderungen für die Bearbeitung besonders schützenswerter Personendaten und nennt folgende Beispiele (hier am Beispiel des Schweizer DSG):

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
- Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
- genetische Daten,

- biometrische Daten, die eine natürliche Person eindeutig identifizieren,
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
- Daten über Massnahmen der sozialen Hilfe.

Ein Beispiel besonders schützenswerter Personendaten im Kontext der Schweizer Museen können Gesundheitsdaten der Mitarbeitenden sein – etwa Informationen zu einer Operation oder einem Case Management der IV.

Handelt es sich um besonders schützenswerte Personendaten, so sind insbesondere die folgenden zusätzlichen Anforderungen zu beachten:

- Für öffentliche Museen sind die Anforderungen an das Legalitätsprinzip erhöht und es bedarf für die Bearbeitung und Bekanntgabe der Daten im Normalfall einer formell-gesetzlichen Grundlage.
- Für private Museen gilt zu beachten, dass für die Bekanntgabe besonders schützenswerter Personendaten ein Rechtfertigungsgrund erforderlich ist und – sofern eine Einwilligung notwendig ist – diese ausdrücklich erfolgen muss (bspw. aktives Ankreuzen eines Kästchens anstatt bereits gesetzte Häkchen).
- Besonders schützenswerte Daten verlangen aufgrund ihrer erhöhten Sensitivität zusätzliche technische und organisatorische Massnahmen, um die Datensicherheit zu gewährleisten.

Bei Anwendbarkeit der kantonalen Datenschutzgesetze muss zudem im Einzelfall geprüft werden, welche zusätzlichen Anforderungen diese für besonders schützenswerte (bzw. häufig auch «besondere Personendaten» genannt) vorsehen.

## 7) Welche Prinzipien sind bei Datenbearbeitungen stets zu beachten?

Das Datenschutzrecht sieht eine Reihe von Grundprinzipien vor, die bei jeder Datenbearbeitung beachtet werden müssen. Man kann sich diese als eine Art «Dach» über allen Datenbearbeitungen vorstellen. Diese Prinzipien werden in diversen Ausführungsbestimmungen im Datenschutzgesetz weiter konkretisiert.

Die *7 Grundprinzipien* lauten wie folgt:

- *Gesetzmässigkeit:* Datenbearbeitungen müssen rechtmässig erfolgen und dürfen nicht gegen geltendes Recht verstossen. Für öffentliche Organe bedeutet es zudem, dass die Bearbeitung gewöhnlicher Personendaten nur basierend auf einer gesetzlichen Grundlage erlaubt ist (oder in gewissen Kantonen: die Datenbearbeitung muss zur Erfüllung einer gesetzlichen Aufgabe notwendig sein). Besondere Personendaten dürfen von öffentlichen Organen nur bei Vorliegen einer formell-gesetzlichen Grundlage bearbeitet werden.

- *Datensparsamkeit*: Nur so viele Personendaten wie nötig! Wenn Daten nicht mehr gebraucht werden, sind sie zu anonymisieren oder zu löschen.

- *Zweckbindung:* Die Personendaten dürfen nur für Zwecke bearbeitet werden, die der betroffenen Person angegeben werden oder die für sie erkennbar sind bzw. die mit dem ursprünglichen Zweck vereinbar sind (Zweckänderungsverbot). Bspw. dürfen Personendaten,

die von Bewerbenden erhoben werden (z.B. Kontaktdaten, Referenzen, CV) nur für den Zweck der Rekrutierung und nicht zusätzlich für einen Newsletter-Versand etc. verwendet werden.

- *Transparenz:* Die betroffenen Personen werden über die Datenbearbeitungen informiert.
- *Datenrichtigkeit:* Unrichtige Daten müssen korrigiert oder gelöscht werden.
- *Sicherheit*: Personendaten müssen vor Verlust, Verfälschung oder unbefugtem Zugriff geschützt werden.
- *Rechenschaftspflicht*: Organisationsintern müssen nötige Prozesse und Verfahren zur Sicherstellung und zum Nachweis der Datenschutzkonformität umgesetzt werden.

## 8) Was versteht man unter Datensicherheit?

Die Datensicherheit ist ein Teilbereich des Datenschutzes. Sie regelt die Verfügbarkeit, Vertraulichkeit, Integrität der bearbeiteten Personendaten sowie die Nachvollziehbarkeit der Datenbearbeitungsvorgänge. Dazu müssen Organisationen geeignete technische und organisatorische Massnahmen ergreifen. Beispiele solcher Massnahmen sind Zugriffskonzepte, Anonymisierungen, Passwort-Schutz, 2-Faktoren-Authentifizierung, Schulungen etc.

Je sensitiver die Personendaten sind, umso höher sind die Anforderungen an die Sicherheitsmassnahmen («Angemessenheit»).

Nebst dem Erfordernis der Datensicherheit im Datenschutz gibt es auch ein breiteres Arbeitsfeld der «Informationssicherheit». Auch hier ist das Ziel, die Verfügbarkeit, Vertraulichkeit und Integrität sicherzustellen; im Gegensatz zum Datenschutz ist der Anwendungsbereich aber breiter. Es geht nicht nur um Personendaten, sondern um alle geschäftsrelevanten Informationen.

Praxistipp: Es empfiehlt sich, die Informationssicherheit und den Datenschutz miteinander so zu verbinden, dass Synergien genutzt und Doppelspurigkeiten vermieden werden können.

## 9) Was ist zu beachten, wenn Datenbearbeitungen an Dritte ausgelagert werden?

Wenn ein Museum bei seiner Tätigkeit Dritte (Unternehmen oder natürliche Personen) beizieht und diese im Rahmen des Auftrags Personendaten bearbeiten, liegt eine sogenannte *Auftragsdatenbearbeitung* vor (bspw. Newsletter-Software oder Kollaborations-Tool von Drittunternehmen).

Die Verantwortung für die Einhaltung des Datenschutzes bleibt dabei stets beim Museum (es ist sog. *Verantwortlicher*). Das Museum muss sicherstellen, dass die Dritten (sog. *Auftragsbearbeitende*) die Daten nur gemäss seinen Weisungen und für die von ihm vorgegebenen Zwecke bearbeiten.

Dazu muss das Museum einen *schriftlichen Vertrag* mit den Auftragsbearbeitenden abschliessen, in welchem es die notwendigen datenschutzrechtlichen Pflichten regelt und überbindet.

## 10) Was ist zu beachten, wenn Personendaten ins Ausland übermittelt werden?

Eine Übermittlung von Personendaten liegt vor, wenn diese physisch im Ausland gespeichert werden (bspw. ausländischer Hosting-Provider) oder Personen aus dem Ausland Zugriff (*remote access)* auf lokal gespeicherte Daten haben (bspw. ausländischer Software-Anbieter in Support-Fällen).

Wenn Personendaten ins Ausland übermittelt werden, so ist ausländische Gesetzgebung auf die Datenbearbeitung anwendbar. Ist diese Gesetzgebung nicht gleichwertig mit dem lokalen Datenschutzrecht, so müssen Schutzmassnahmen getroffen werden. Dabei wird nach folgender Kaskade vorgegangen:

1. *Sicherer Drittstaat*: Als Land mit genügendem Datenschutzniveau gelten z.B. alle Staaten des EWR-Raums (sichere Drittstaaten), nicht aber die USA, China oder Russland (unsichere Drittstaaten). Bei Übermittlung in sichere Drittstaaten sind keine Zusatzmassnahmen notwendig.

2. *Geeignete Schutzmassnahmen:* Bei Übermittlung in unsichere Drittstaaten müssen zusätzliche Massnahmen getroffen werden, bspw. sind von der Datenschutzaufsicht genehmigte Datenschutzklauseln oder die Standarddatenklauseln der EU-Kommission abzuschliessen.

3. *Ausnahmegrund:* Ohne geeignete Schutzmassnahmen können Daten nur in Ausnahmefällen ins Ausland übermittelt werden. Dies, wenn bspw. eine ausdrückliche Einwilligung vorliegt oder die Bekanntgabe zur Wahrung überwiegender Interessen notwendig ist.

## 11) Was ist eine Datenschutz-Folgenabschätzung und wie wird sie durchgeführt?

Wie der Name sagt, ist die Datenschutz-Folgenabschätzung ein Nachdenken über die Risiken einer Datenbearbeitung, die man dokumentiert. Das Datenschutzgesetz sieht vor, dass die Auswirkungen einer Datenbearbeitung auf die betroffenen Personen immer vorab zu prüfen sind, und zwar bei jedem neuen Projekt, das die Bearbeitung von Personendaten mit sich bringt, sowie wenn eine bestehende Datenbearbeitung angepasst wird.

Es werden die beabsichtigte Datenbearbeitung, die Bearbeitungszwecke, die betroffenen Daten- und Personenkategorien, mögliche Risiken und risikomitigierende Massnahmen und eine Reihe weiterer Informationen dokumentiert.

Falls trotz der Umsetzung von Schutzmassnahmen hohe Risiken für die Grundrechte der betroffenen Personen verbleiben (bspw. bei umfangreiche Datenbearbeitungen oder beim Einsatz von Videoüberwachungs-Software mit Analysefunktionen), so muss die Datenschutz-Folgenabschätzung der jeweiligen eidgenössischen oder kantonalen Datenschutzaufsicht zur Beurteilung vorgelegt werden.

Für den Kanton Zürich empfiehlt sich, das Merkblatt und Formular der Datenschutzbeauftragten des Kantons Zürich zu verwenden (https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutz-folgenabschaetzung).

## 12) Was ist zu tun, wenn die Datensicherheit verletzt wurde?

Die Museen müssen Verletzungen der Datensicherheit intern analysieren und der eidgenössischen oder kantonalen Datenschutzaufsicht im Normalfall dann melden, wenn daraus ein hohes Risiko für die Grundrechte der betroffenen Personen resultiert (*data breach notification*). Nota bene: In gewissen kantonalen Gesetzen ist die Schwelle etwas tiefer angesetzt und Datenschutzvorfälle sind immer zu melden.

Eine Verletzung der Sicherheit liegt vor, wenn die Integrität, Vertraulichkeit, Verfügbarkeit oder Nachvollziehbarkeit der Daten nicht mehr gewährleistet ist und Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Das ist bspw. der Fall, wenn ein USB-Stick oder Geschäfts-Computer verloren geht oder liegen gelassen wird, bei Cyberangriffen (DDoS-Attacke, Phishing) oder Datenzugriffen durch unberechtigte Personen.

Alle Mitarbeitenden der Museen müssen jeden Verdacht auf einen Datenschutzvorfall intern bei einer dafür designierten Stelle – idealerweise die Sicherheitsbeauftragte oder der Datenschutzberater - unverzüglich (!) melden. Intern ist dann zu analysieren und dokumentieren, ob ein Datenschutzvorfall im Sinne des Gesetzes vorliegt. Ist dies der Fall, sind folgende Schritte notwendig:

- Ergreifen von Massnahmen zur Risikoeindämmung
- Unverzügliche Meldung an Datenschutzaufsicht (innert 72 Stunden gemäss Praxis bzw. je nach kantonalen datenschutzrechtlichen Bestimmungen)
- Information an die betroffene Person, wenn der Datenschutzvorfall für sie ein grosses Risiko bedeutet oder sie selber Schutzmassnahmen treffen muss (bspw. Wechsel des Passwortes)

Für Meldungen von Zürcher Museen kann das von der Datenschutzbeauftragten des Kantons Zürich zur Verfügung gestellte Formular verwendet werden (https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutzvorfall-melden).

## 13) Was geschieht, wenn Datenschutzbestimmungen missachtet werden?

Der Schutz der Personendaten ist nicht freiwillig, sondern gesetzlich vorgeschrieben.

Zuständige Datenschutzaufsicht für die Schweizer Museen sind entweder der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) oder die kantonalen Datenschutzbehörden (vgl. eine Übersicht auf https://www.privatim.ch/de/privatim/). Sie überwachen die Anwendung der Datenschutzvorschriften und haben Kontrollbefugnisse (z.B. Recht auf Auskunft oder Einsichtnahme), können Empfehlungen abgeben oder die Anpassung oder Einstellung von Datenbearbeitungen verfügen.

Neben Aufsichtsmassnahmen können die betroffenen Personen Datenschutzverletzungen auf zivil- oder verwaltungsrechtlichem Weg direkt beim Museum geltend machen und bspw. die Beendigung oder Beseitigung widerrechtlicher Datenbearbeitungen verlangen. Bei finanziellem Schaden oder schwerer Persönlichkeitsverletzung hat die betroffene Person sodann Anspruch auf Schadenersatz oder Genugtuung.

Nach dem Schweizer Datenschutzgesetz drohen sodann strafrechtliche Sanktionen für private Personen (konkret Mitarbeitende) und Bussen von bis zu CHF 250'000.00. Die Strafbarkeit ist jedoch nur für gewisse Datenschutzpflichten vorgesehen und verlangt mindestens Eventualvorsatz. Eventualvorsatz bedeutet, dass die Datenschutzverletzung zwar nicht bewusst angestrebt, jedoch in Kauf genommen wird.

Nebst diesen rechtlichen Sanktionen kann die Nichteinhaltung des Datenschutzrechts schwere Reputationsrisiken in sich bergen.

***